UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/562,543	12/28/2005	Thomas Andreas Maria Kevenaar	NL030858	6017

24737 7590 08/19/2008
PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
POGMORE, TRAVIS D	

ART UNIT	PAPER NUMBER
4148	

MAIL DATE	DELIVERY MODE
08/19/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/562,543	KEVENAAR, THOMAS ANDREAS MARIA	
	Examiner	Art Unit	
	TRAVIS POGMORE	4148	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 December 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *28 December 2005, 09 May 2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The instant application having Application No. 10/562543 filed on December 28, 2005 is presented for examination by the examiner.

Oath/Declaration

2. The applicant's oath/declaration has been reviewed by the examiner and is found to conform to the requirements prescribed in 37 C.F.R. 1.63.

Priority

3. As required by M.P.E.P. 201.14(c), acknowledgement is made of applicant's claim for priority based on applications filed on July 3, 2003 (EP Application No. 03101998.7).

4. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Information Disclosure Statement

5. As required by M.P.E.P. 609, the applicant's submissions of the Information Disclosure Statement dated May 8, 2007 is acknowledged by the examiner and the cited references have been considered in the examination of the claims now pending.

Drawings

6. The applicant's drawings submitted are acceptable for examination purposes.

Claim Rejections – 35 USC § 112

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claim 5 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 5 recites the limitation "the sender device" in line 4. There is insufficient antecedent basis for this limitation in the claim.

As described in the disclosure and later in claim 7, the sender device is not comprised of group identities, but protecting means to add a MIC and transmitting means. The notion as written of it comprising an abstract concept such as a group identity is nonsensical and renders the claim meaningless.

Claim Rejections – 35 USC § 101

9. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

10. Claim 11 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter because of the following reason:

11. The claim fails to place the invention squarely within one statutory class of invention. Claim 11 is a signal *per se*. As such, the claim is drawn to a form of energy. Energy is not one of the four categories of invention and therefore this claim is not

statutory. Energy is not a series of steps or acts and thus is not a process. Energy is not a physical article or object and as such is not a machine or manufacture. Energy is not a combination of substances and therefore not a composition of matter.

Claim Rejections – 35 USC § 102

12. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

13. Claims 7-8 and 10 are rejected under 35 U.S.C. 102(b) as being anticipated by WIPO Publication No. WO-2000/062503 A2 (hereinafter "Hardjono").

As to claim 7, Hardjono teaches a sender device (page 3, lines 13-17, the "network device") being arranged to transmit a communication fragment through a router device towards a receiver device, the communication fragment comprising a first target address reference referring to a group of at least one receiver device (page 3, lines 20-22 and 25-27, the nature of multicasts is such that they include group addresses), the sender device comprising:

- protecting means being arranged to add a cryptographic message integrity code to protect at least part of the communication fragment (page 3, lines 15-17, the "tag generator"), and

- transmitting means begin arranged to transmit the communication fragment to a router device that is not able to modify the cryptographic message integrity code (page 8, line 29 through page 9, line 2, routers in Hardjono act as routers, senders and receivers and in the embodiment described merely append tags/MICs instead of changing them).

As to claim 8, Hardjono teaches a router device (page 5, lines 9-10) being arranged to route a communication fragment from a sender device towards a receiver device, the communication fragment comprising a first target address reference referring to a group of at least one receiver device (page 5, lines 10-13), the router device comprising:

- receiving means being arranged to receive the communication fragment, comprising a first address reference referring to a group of at least one receiver device, the first communication fragment at least partly being protected by a MIC (page 5, lines 10—13 and 16-18, the processing hardware and software recited on line 11 relies on the identification tags (as indicated on page 3, lines 17-22) to authenticate the messages, so these must be a part of the received and transmitted messages),

- modifying means being arranged to modify the communication fragment, by replacing the group of at least one receiver device by a reference referring to the at least one receiver device, while maintaining the original MIC (page 8, line 29 through page 9, line 2, the router ID number of the receiving router being appended to the message/base tag combination), and

- transmitting means to transmit the modified communication fragment to the at least one receiver device (page 9, lines 7-9, routers in Hardjono act as routers, senders and receivers).

As to claim 10, Hardjono teaches a system for communication comprising a sender device, router device, and receiver device as described in claim 7 (page 3, lines 24-29).

Claim Rejections – 35 USC § 103

14. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

15. Claims 1-3, 5-6, 9 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hardjono in view of European Patent Application Pub. No. EP 1032178 A1 (hereinafter "Chen et al.").

As to claim 1, Hardjono teaches a method of communicating a communication fragment, the communication fragment comprising a first target address reference referring to a group of at least one receiver device (Fig. 4, as described on page 4, lines 29-30), comprising the steps of:

- a sender device adding a cryptographic message integrity code to protect at least part of the communication fragment (Fig. 4, element 404),

- the sender device transmitting the protected communication fragment to a router device (Fig. 4, element 406),

Hardjono does not specifically teach the router device, for at least one receiver device in the group of target devices, modifying the first target address reference into an address of the at least one receiver device, while maintaining the unchanged cryptograph message integrity code, and subsequently forwarding the modified protected communication fragment to the at least one receiver device,

the at least one receiver device receiving the modified protected communication fragment,

the at least one receiver device restoring the original protected communication fragment in order to allow verification of the original protected communication fragment using the message integrity code.

However, Chen et al. teaches the router device, for at least one receiver device in the group of target devices, modifying the first target address reference into an address of the at least one receiver device, while maintaining the unchanged cryptograph message integrity code, and subsequently forwarding the modified protected communication fragment to the at least one receiver device (column 10, lines 7-21 and column 11, line 58 through column 12, line 12, the home agent acts as the router device and suggests that it may be necessary to amend any error checking while

not mandating that the home agent does so, and the foreign agent acts as a receiver device),

the at least one receiver device receiving the modified protected communication fragment (column 12, lines 2-12),

the at least one receiver device restoring the original protected communication fragment in order to allow verification of the original protected communication fragment using the message integrity code (column 12, lines 2-12).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the teaching of Hardjono to include the router device directly modifying the target address reference and the receiver device restoring the original protected communication of Chen et al. because this would avoid longer communication fragments normally needed (Chen et al., column 3, lines 25-34).

As to claim 2, Hardjono and Chen et al. do not specifically teach wherein the first communication fragment comprises a bit field IA to indicate whether indirect addressing is used.

However, the concept and advantages of using a bit field to indicate whether an indirect address is being used is well known and expected in the art. For example U.S. Patent App. Pub. US 2003/0223402 A1 (page 2, paragraph 30, multicast by its nature uses indirect addressing).

Therefore it would have been obvious to a person having ordinary skill in the art at the time of the invention was made to modify the teaching of Hardjono and Chen et al. to use a single bit to indicate whether or not indirect addressing was being used.

As to claim 3, Hardjono teaches wherein the sender device and the at least one receiver device share a common cryptographic key, and where the cryptographic message integrity code is computable and verifiable only by using the common cryptographic key (page 6, lines 12-13 and 19-20).

As to claim 5, Hardjono and Chen et al. teach wherein the at least one receiver device restores the original protected communication fragment by substituting the first target address reference with each of the group identities (Chen et al., column 12, lines 4-12) that comprises the sender device to determine for which of the group identities the message integrity code matches (Hardjono, page 3, lines 17-22).

As to claim 6, Chen et al. teaches wherein

- the router device, in the step of modifying the first target address reference, stores the first target address reference in the modified protected communication fragment (column 11, lines 48-57), and

- the at least one receiver device restores the original protected communication fragment using the stored first target address reference in the modified protected communication fragment in order to allow verification of the message integrity code

(column 12, lines 2-12, the restored mobile nodes home address returns the communication fragment/IP packet to it's original state which is what's required for MIC verification).

As to claim 9, Hardjono teaches verification means being arranged to verify the cryptographic message integrity code (page 3, lines 13-20, the authenticator reading and authenticating the tags to determine message origin applies equally to MICs).

Hardjono does not specifically teach a receiver device being arranged to receive a modified communication fragment originating from a transmitter device through a router device, the modified communication fragment being derived from a communication fragment comprising a first target address reference referring to a group of at least one receiver, the receiver device comprising:

- receiving means being arranged to receive the modified communication fragment, and

- restoring means being arranged to restore the original communication fragment that was used to compute the cryptographic message integrity code.

However, Chen et al. teaches a receiver device being arranged to receive a modified communication fragment originating from a transmitter device through a router device, the modified communication fragment being derived from a communication fragment comprising a first target address reference referring to a group of at least one receiver device (column 10, lines 7-21, a care-of address for a single node is a group of

at least one receiver device, this is also standard practice for multicast in general), the receiver device comprising:

- receiving means being arranged to receive the modified communication fragment (column 12, lines 2-4), and

- restoring means being arranged to restore the original communication fragment that was used to compute the cryptographic message integrity code (column 12, lines 4-8).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the teaching of Hardjono to include the receiver device as in Chen et al. being arranged to receive communication fragments and the means to restore them to their original state used to compute the MIC as in Hardjono, because this would allow care-of and multicast addressing to still utilize an original MIC.

As to claim 11, Hardjono teaches a signal for secure indirect addressing, comprising a modified communication fragment according to the method of claim 1 (Hardjono, page 13, lines 7-13, the "wireless techniques" mentioned include signals).

16. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hardjono in view of Chen et al. and further in view of US Patent Application Pub. No. US 20020078353 A1 (hereinafter "Sandhu").

As to claim 4, Hardjono and Chen et al. do not specifically teach wherein the common cryptographic key is used to encrypt the message content.

However, Sandhu teaches wherein the common cryptographic key is used to encrypt the message content (page 1, paragraphs 9-10).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the teaching of Hardjono in view of Chen et al. to use the common cryptographic key to encrypt the message content of Sandhu, because this would avoid the need to generate, distribute, and store multiple common cryptographic keys to allow both message integrity verification and message encryption.

Conclusion

17. The following prior art made of record and not relied upon is cited to establish the level of skill in the applicant's art and those arts considered reasonably pertinent to applicant's disclosure. See MPEP 707.05(c).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TRAVIS POGMORE whose telephone number is (571)270-7313. The examiner can normally be reached on Monday through Thursday between 7:30 a.m. and 5:00 p.m. eastern time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Thomas Pham can be reached on 571-272-3689. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/THOMAS PHAM/
Supervisory Patent Examiner, Art Unit 4148

/T. P./
Examiner, Art Unit 4148